Теорема Эйлера

Теорема 15

Пусть $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. *Тогда* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Доказательство. • Пусть $r_1, \ldots, r_{\varphi(m)}$ — ПрСВ $\pmod{m}$.

• По Теореме 14 тогда и $ar_1, \ldots, ar_{\varphi(m)}$ — ПрСВ $\pmod{m}$.

• Введем обозначения i_1, ..., $i_{\varphi(m)}$ так, что $r_1 \equiv_m ar_{i_1}$, ..., $r_{\varphi(m)} \equiv_m ar_{i_{\varphi(m)}}$ и $\{1, \ldots, \varphi(m)\} = \{i_1, \ldots, i_{\varphi(m)}\}$.

• Пусть $R = r_1 \cdot \cdots \cdot r_{\varphi(m)}$. Тогда $(R, m) = 1$.

• Перемножая записанные выше сравнения, получаем

$$R \equiv r_1 \cdot \cdots \cdot r_{\varphi(m)} \equiv ar_1 \cdot \cdots \cdot ar_{\varphi(m)} \equiv a^{\varphi(m)} \cdot R \pmod{m}.$$

Сокращая на R, получаем $1 \equiv a^{\varphi(m)} \pmod{m}$. □

Функция Эйлера

Лемма 4

Функция Эйлера мультипликативна, то есть, если $a, b \in \mathbb{N}$ взаимно просты, то $\varphi(ab) = \varphi(a)\varphi(b)$.

Доказательство. • Запишем числа от 1 до ab в таблицу $a \times b$ так, что в первой строке — числа от 1 до a, во второй — от $a + 1$ до $2a$, итд, в b строке — числа от $(b - 1)a + 1$ до ba.

• Все числа в i столбце принадлежат одному вычету $\bar{i} = i + a\mathbb{Z}$ по модулю a. Эти числа взаимно просты с a, если и только если $(i, a) = 1$.

• Вычеркнем все столбцы с номерами i, не взаимно простыми с a. Останутся ровно $\varphi(a)$ столбцов.

• Все числа, взаимно простые с ab, должны быть взаимно простыми и с a, они лежат в оставшихся $\varphi(a)$ столбцах.

• Рассмотрим оставшийся столбец, пусть числа в нем имеют вид $j,\ a + j,\ \dots,\ (b - 1)a + j$. Эти числа образуют ПСВ $\pmod{b}$ в силу теоремы 13 (так как получены из ПСВ $0,1,\dots,b-1$ умножением на a, взаимно простое с b и прибавлением j: $\quad 0 \to j,\ 1 \to a + j,\ \dots,\ b - 1 \to (b - 1)a + j$).

• Значит, среди чисел $j,\ a + j,\ \dots,\ (b - 1)a + j$ ровно $\varphi(b)$ взаимно простых с b. Остальные числа точно не взаимно просты с ab, вычеркнем их.

• Оставшиеся $\varphi(a)\varphi(b)$ чисел взаимно просты и с a, и с b, а значит, взаимно просты с ab. Значит, осталось ровно $\varphi(ab)$ чисел (все числа от 1 до ab, взаимно простые с ab). $\square$